

This site uses cookies. By continuing to browse the site you are agreeing to our use of cookies. [Find out more here](#)

the **guardian**

Search

US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data

- 2007 deal allows NSA to store previously restricted material
- UK citizens not suspected of wrongdoing caught up in dragnet
- Separate draft memo proposes US spying on 'Five-Eyes' allies

Follow The NSA Files by email **BETA**

James Ball

The Guardian, Wednesday 20 November 2013 14.00 EST

(S//SI//REL) SID Analysts Can Now Unminimize

FROM: [REDACTED]
SIGINT Policy (S02L1)
Run Date: 05/16/2007

(S//SI//REL) SIGINT Policy (S02L1) and the UK Liaison Office here at NSA have been instructed to unminimize UK data incidentally collected in SIGINT analysis. The new policy allows for the unminimizing of incidentally collected UK phone numbers for use in analysis. This includes contact identifiers, including IP and email addresses, fax and cell phone numbers, for

- (S//SI//REL) Are authorized to unmask UK contact identifiers resulting from communications collected/selected incidental to the original SIGINT task.

The memo explains that the US and UK 'worked together to come up with a new policy that expands the use of incidentally collected unminimized UK data.'

The phone, internet and email records of UK citizens not suspected of any wrongdoing have been analysed and stored by America's National Security Agency under a secret deal that was approved by British intelligence officials, according to documents from the whistleblower Edward Snowden.

In the first explicit confirmation that UK citizens have been caught up in US mass surveillance programs, an NSA memo describes how in 2007 an agreement was reached that allowed the agency to "unmask" and hold on to personal data about Britons that had previously been off limits.

The memo, published in a joint investigation by the Guardian and Britain's Channel 4 News, says the material is being put in databases where it can be made available to other members of the US intelligence and military community.

Britain and the US are the main two partners in the 'Five-Eyes' intelligence-sharing alliance, which also includes Australia, New Zealand and Canada. Until now, it had been generally understood that the citizens of each country were protected from surveillance by any of the others.

But the Snowden material reveals that:

- In 2007, the rules were changed to allow the [NSA](#) to analyse and retain any British citizens' mobile phone and fax numbers, emails and IP addresses swept up by its dragnet. Previously, this data had been stripped out of NSA databases – "minimized", in intelligence agency parlance – under rules agreed between the two countries.
- These communications were "incidentally collected" by the [NSA](#), meaning the individuals were not the initial targets of surveillance operations and therefore were not suspected of wrongdoing.
- The NSA has been using the UK data to conduct so-called "pattern of life" or "contact-chaining" analyses, under which the agency can look up to three "hops" away from a target of interest – examining the communications of a friend of a friend of a friend. [Guardian analysis suggests](#) three hops for a typical Facebook user could pull the data of more than 5 million people into the dragnet.
- A separate draft memo, marked top-secret and dated from 2005, reveals a proposed NSA procedure for spying on the citizens of the UK and other [Five-Eyes](#) nations, even where the partner government has explicitly denied the US permission to do so. The memo makes clear that partner countries must not be informed about this surveillance, or even the procedure itself.

The 2007 briefing was sent out to all analysts in the NSA's Signals Intelligence Directorate (SID), which is responsible for collecting, processing, and sharing information gleaned from US surveillance programs.

Up to this point, the Americans had only been allowed to retain the details of British landline phone numbers that had been collected incidentally in any of their trawls.

But the memo explains there was a fundamental change in policy that allowed the US to look at and store vast amounts of personal data that would previously have been discarded.

It states: "[Sigint](#) [signals intelligence] policy ... and the UK Liaison Office here at NSA [NSA Washington] worked together to come up with a new policy that expands the use of incidentally collected unminimized UK data in Sigint analysis.

"The new policy expands the previous memo issued in 2004 that only allowed the unminimizing of incidentally collected UK phone numbers for use in analysis.

"Now SID analysts can unminimize all incidentally collected UK contact identifiers, including IP and email addresses, fax and cell phone numbers, for use in analysis."

The memo also set out in more detail what the NSA could and could not do.

The agency was, for example, still barred from making any UK citizen a target of surveillance programs that would look at the content of their communications without getting a warrant. However, they now:

- "Are authorized to unmask UK contact identifiers resulting from incidental collection."
- "May utilize the UK contact identifiers in [Sigint](#) development contact chaining analysis."
- "May retain unminimized UK contact identifiers incidentally collected under this authority within content and [metadata](#) stores and provided to follow-on USSS (US Sigint System) applications."

The document does not say whether the UK Liaison Office, which is operated by [GCHQ](#), discussed this rule change with government ministers in London before granting approval, nor who within the intelligence agencies would have been responsible for the decision.

The Guardian contacted [GCHQ](#) and the Cabinet Office on Thursday November 7 to ask for clarification, but despite repeated requests since then, neither has been prepared to comment.

Since the signing in 1946 of the UKUSA Signals Intelligence Agreement, which first established the Five-Eyes partnership, it has been a convention that the allied intelligence agencies do not monitor one another's citizens without permission – an agreement often referred to publicly by officials across the Five-Eyes nations.

However, a draft 2005 directive in the name of the NSA's director of signals intelligence reveals the NSA prepared policies enabling its staff to spy on Five-Eyes citizens, even where the partner country has refused permission to do so.

a) (S//SI//NF) Under the British-U.S. Communications Intelligence Agreement of 5 March 1946 (commonly known as the United Kingdom/United States of America (UKUSA) Agreement), both governments agreed to exchange communications intelligence products, methods and techniques as applicable so long as it was not prejudicial to national interests. This agreement has evolved to include a common understanding that both governments will not target each other's citizens/persons. However, when it is in the best interest of each nation, each reserved the right to conduct unilateral COMINT action against each other's citizens/persons. Therefore, under certain circumstances, it may be advisable and allowable to target Second Party persons and second party communications systems unilaterally when it is in the best interests of the U.S. and necessary for U.S. national security. Such targeting must be performed exclusively within the direction, procedures and decision processes outlined in this directive.

The document, titled 'Collection, Processing and Dissemination of Allied Communications', has separate classifications from paragraph to paragraph. Some are cleared to be shared with America's allies, while others – marked "NF", for No Foreign – are to be kept strictly within the agency. The NSA refers to its Five-Eyes partners as "second party" countries.

The memo states that the Five-Eyes agreement "has evolved to include a common understanding that both governments will not target each other's citizens/persons".

But the next sentence – classified as not to be shared with foreign partners – states that governments "reserved the right" to conduct intelligence operations against each other's citizens "when it is in the best interests of each nation".

"Therefore," the draft memo continues, "under certain circumstances, it may be advisable and allowable to target second party persons and second party communications systems unilaterally, when it is in the best interests of the US and necessary for US national security."

The draft directive states who can approve the surveillance, and stresses the need for secrecy.

b) (S//NF) Unilaterally by the Signals Intelligence Directorate:
When sharing the planned targeting information with a Second Party would be contrary to U.S. interests, or when the Second Party declines a collaboration proposal, the proposed targeting must be presented to the Signals Intelligence Director for approval with justification for the criticality of the proposed collection. If approved, any collection, processing and dissemination of the Second Party information must be maintained in NOFORN channels.

"When sharing the planned targeting information with a second party would be contrary to US interests, or when the second party declines a collaboration proposal, the proposed targeting must be presented to the signals intelligence director for approval with justification for the criticality of the proposed collection.

"If approved, any collection, processing and dissemination of the second party information must be maintained in

NoForn channels."

The document does not reveal whether such operations had been authorized in the past, nor whether the NSA believes its Five-Eyes partners conduct operations against US citizens.

The other sections of the document, cleared for sharing with the UK and other partners, strike a different tone, emphasising that spying on each other's citizens is a collaborative affair that is most commonly achieved "when the proposed target is associated with a global problem such as weapons proliferation, terrorism, drug trafficking or organised crime activities."

It states, for example: "There are circumstances when targeting of second party persons and communications systems, with the full knowledge and co-operation of one or more second parties, is allowed when it is in the best interests of both nations."

b) (S//SI//REL to UK, CAN, AUS, NZ and USA) There are circumstances when targeting of Second party persons and communications systems, with the full knowledge and cooperation of one or more Second Parties, is allowed when it is in the best interests of both nations. This targeting will conform to guidelines set forth in this directive.

The memo says the circumstances might include "targeting a UK citizen located in London using a British telephone system"; "targeting a UK person located in London using an internet service provider (ISP) in France; or "targeting a Pakistani person located in the UK using a UK ISP."

A spokeswoman for the NSA declined to answer questions from the Guardian on whether the draft directive had been implemented and, if so, when. The NSA and the White House also refused to comment on the agency's 2007 agreement with the UK to store and analyze data on British citizens.

The British foreign secretary in 2005 was Jack Straw, and in 2007 it was Margaret Beckett. The Guardian approached both of them to ask if they knew about or sanctioned a change in policy. Both declined to comment.

The Five-Eyes nations have, so far, steered clear of the diplomatic upheavals, which have emerged as a result of revelations of the NSA spying on its allies.

France, Germany and Spain have all recently summoned their respective US ambassadors to discuss surveillance within their borders, while earlier this month the UK ambassador to Germany was invited to discuss alleged eavesdropping from the UK embassy in Berlin.



Get the Guardian's daily US email

Our editors' picks for the day's top news and commentary delivered to your inbox each morning.

[Sign up for the daily email](#)

More from the Guardian

[What's this?](#)



Why it's a good time to be a dictator like Kim Jong-un

Hollie Gazzard attack was filmed by bystanders, say police

Image of Syrian boy in desert triggers sympathy — and then a backlash

UK floods: troops could have been deployed earlier Philip Hammond says

More from around the web



The 10 Largest Combat Air Forces in the World (The Richest)



Building A Timeless Wardrobe (THE LINE)



Yes, These 20 Weirdest Animals on the Planet Do Exist (Rant Lifestyle)



13 Secrets A Flight Attendant Will Never Tell You! (Reader's Digest)

Ads by Google

[Escape from America](#)

6 Places to Protect and Grow Your Wealth as US Spirals Out of Control

www.sovereign-investor.com

[Concealed Carry Guide](#)

Limited Time Free Subscription Get Informed & Stay Safe!

usconcealedcarry.net

[How to Fix Slow Computer](#)

Easily Repair a Slow Computer! Very Simple Instructions (Recommended)

windowsanswers.net/Slow-Computer

© 2014 Guardian News and Media Limited or its affiliated companies. All rights reserved.

;